#20
1/3

JRM:lmp 5/31/01 50848

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Geoffrey B. Rhoads

Filed: November 5, 1998

For: METHOD FOR MONITORING INTERNET DISSEMINATION OF IMAGE, VIDEO AND/OR AUDIO FILES

Examiner: J. Couso

Date: May 30, 2001

Response Under 37 CFR § 1.116
Expedited Procedure
Art Unit 2721

CERTIFICATE OF MAILING

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being deposited with the United States Postal Service on May 31, 2001 as First Class Mail in an envelope addressed to: BOX AF ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231.

Joel R. Meyer
Attorney for Applicant

APPEAL BRIEF

BOX AF
ASSISTANT COMMISSIONER FOR PATENTS
Washington, DC 20231

Sir:

This brief is in furtherance of the Notice of Appeal filed February 21, 2001. The fee required under 37 CFR 1.17(f) is enclosed. Please charge any deficiency to deposit account 50-1071.

06/06/2001 GTEFFERA 00000144 501071 09186962
02 FC:120 310.00 CH

I. REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation, by an assignment from the inventor recorded at Reel 8050, Frames 0932-0934, on July 29, 1996.

II. RELATED APPEALS AND INTERFERENCES

Applicant has requested interferences in co-pending applications 09/538,493 and 09/657,148, but none has been declared.

III. STATUS OF CLAIMS

Claims 2-21 are finally rejected and appealed.

IV. STATUS OF AMENDMENTS

All earlier-filed amendments have been entered.

V. SUMMARY OF THE INVENTION

The invention relates to methods of monitoring distribution of proprietary audio or image files on the Internet using steganographically embedded data, such as digital watermarks embedded in the image or audio data. See claim 2, 19-21 in the Appendix.

Steganography refers to hiding a message within other, empirical data. See specification, page 59, lines 7-9. See also enclosed excerpt from Johnson, Neil F. et al. "Information Hiding - Steganography and Watermarking – Attacks and Countermeasures", 2001, Preface and Ch. 1 pages 1 –2. Digital watermarking is a form of steganography in which auxiliary data is embedded substantially imperceptibly in electronic media signals like audio and image signals (still images and video). See Background section in specification, pages 1-3; and the various embodiments in the specification for embedding auxiliary data in audio and image signals.

Distribution of imagery (including, e.g., graphics and video) and audio on the Internet is quick and simple. While advantageous in most respects, this ease of distribution makes it difficult for proprietors of such materials to track the uses to which their

audio/imagery/graphics/video are put. It also allows such properties to be copied illicitly, in violation of the proprietors' copyrights.

Embodiments of the invention seek to redress these drawbacks by monitoring Internet dissemination of various properties, and reporting the results back to their proprietors. If an unauthorized copy of a work is detected, appropriate steps can be taken to remove the copy, or compensate the proprietor accordingly. See Specification page 80, lines 16-35.

In accordance with one embodiment of the present invention, a monitoring system downloads various image files (including video or graphic files) or audio files over the Internet, and identifies some as having embedded digital watermark data. The system decodes such watermark data and, from the decoded data, determines the proprietor of each file. The proprietors are then alerted to the results of the monitoring operation, informing them about otherwise unknown distribution of their image/audio properties. See Specification page 80, lines 16-35. See also Specification page 32, lines 6-17; page 35, lines 22-34; page 48, line 33 to page 56, line 19; and page 81, line 1 to page 87, line 19.

In some embodiments, the proprietorship is determined by reference to a registry database, in which a watermarked identification code is associated with textual information identifying the proprietor of a work. See Specification page 60, lines 7-16. See also, Specification page 102, lines 1-11.

Some embodiments perform a domain transformation on the image or audio data in files as part of the process of identifying files that have embedded digital watermark data. See, for example, Specification at page 51, line 31 to 52, line 10; page 84, lines 18-19, page 86, lines 6-36, page 103, lines 1-5, and Appendix B, computer program listing Align.cpp. Examples of this domain transformation include a 2D FFT transform, a one-dimensional transform, and a Fourier Mellin transform. Further, some embodiments perform a matched filtering operation on the transformed data.

In some embodiments, the digital watermark data is decoded using public key data, while in others, it is decoded with private key data. See, for example, the discussion of keys and their relationship to embedded codes at Specification, page 31, line 31 to page 32, line 30. See the discussion of private and public codes at Specification page 58, lines 1-10, page 80, lines 16-19.

In some embodiments, various types of screening operations can be applied to the downloaded files to identify those most likely to contain embedded watermark data, so that complete watermark detection operations are performed only on a subset of the downloaded files. See, for example, Specification page 35, lines 23-34; page 51, line 31 to 52, line 10; page 83, line 35 to page 84, line 5.

VI. ISSUE

- Did the Office establish a prima facie case of obviousness in rejecting claims 2-21 as obvious over U.S. Patent No. 5,721,788 to Powell in view of U.S. Patent No. 4,977,594 to Shear, when (a) the references – collectively – fail to detail all of the elements claimed, and (b) there is no teaching or suggestion in the art that would have led an artisan to modify and combine the references as proposed?

VII. GROUPING OF CLAIMS

The independent claims, 2, 19 and 21 and the dependent claims, 3 – 18, are independently patentable. Claim 20 stands or falls with claim 19.

VIII. ARGUMENT

1. Discussion of Powell (5,721,788)

Powell discloses:

"...a method and system for embedding image signatures within visual images, applicable in the preferred embodiments described herein to digital representations as well as other media such as print or film. The signatures identify the source or ownership of images and distinguish between different copies of a single image. In preferred embodiments, these signatures persist through image transforms such as resizing and conversion to or from print or film and so provide a method to track subsequent use of digital images including derivative images in print or other form." Powell at Col. 1., lines 43-53.

In the detailed description, Powell discloses:

> ...a method and system for embedding a signature into an original image to create a signed image. A preferred embodiment includes selecting a large number of candidate points in the original image and selecting a number of signature points from among the candidate points. The signature points are altered slightly to form the signature. The signature points are stored for later use in auditing a subject image to determine whether the subject image is derived from the signed image. Powell at Col. 2, lines 34-42.

Cols. 5-7 of Powell describe a process of auditing an image.

First, the signature embedded in an image is stored in a database as follows:

> "In order to allow future auditing of images to determine whether they match the signed image, the signature is stored in a database in which it is associated with the original image. The signature can be stored by associating the bit value of each signature point together with x-y coordinates of the signature point. The signature may be stored separately or as part of the signed image. The signed image is then distributed in digital form." Powell at col. 5, lines 21-28.

An original image is then identified "of which the subject image is suspected of being a duplicate." Powell at col. 5, lines 45-46.

Next, Powell describes that:

> "The subject digital image is normalized using techniques as described below to the same size, and same overall brightness, contrast and color profile as the unmodified original image. The subject image is analyzed by the method described below to extract the signature, if present, and compare it to any signatures stored for that image." Powell at col. 5 lines 49-54.

Next, Powell describes that the original image or the original signed image is used to get signature points. See Powell at Col. 6 line 44 to Col. 7, line 14.

Powell explains that the signature points are used to determine whether the subject image was derived from the signed image:

> "These signature points, if any, are compared to the stored signature points for the signed image. If the signature points do not match, then the subject image is not an image derived from the signed image, unless the subject image was changed substantially from the signed image." Powell at Col. 6, lines 48-53.

In summary, Powell's preferred embodiment describes an auditing process where:

1. the original image is identified, of which the subject image is suspected of being a duplicate; Powell at col. 5, lines 45-46; and

2. the subject image is analyzed to extract a signature, if present, and compare it to any signatures stored for that particular image. Powell at col. 5, lines 52-54.

3. the auditing process indicates whether or not the subject image was derived from the signed image. Powell at col. 6, lines 50-53.

The Final Rejection asserts that Powell describes each of the elements of the pending claims, except that "Powell does not specifically state that the system is obtaining audio or image files from plural different Internet sites." The Final Rejection goes on to state that this process is well known in the art. See Final Rejection, page 3.

In rejecting the pending claims, the Final Rejection repeats the claim language and cites portions of Powell that purportedly describe the cited claim language. As set forth in detail below, Applicant respectfully submits that the combined teachings of Powell and Shear do not disclose, teach or suggest the claimed subject matter.

2. Discussion of Shear (4,977,594)

According to the final rejection, "Shear discloses a data base usage metering and protection system and method which specifically discusses the obtaining [of] audio or image files from plural different Internet sites." See Final Rejection at page 3.

Shear does not disclose any method of steganography or digital watermarking. The Final Rejection only relies on Shear as a reference that purportedly shows obtaining files from the Internet. Specifically, this purported teaching is discussed in connection with claim 2 (page 3 of Final Rejection), claim 16 (page 5 of Final Rejection), claims 19-20 (page 7 of the Final Rejection) and claim 21 (page 8 of the Final Rejection).

On page 9, the Final Rejection states that Shear is only relied on as a secondary reference to show a system of obtaining audio or image files from plural different Internet sites. The only portion of Shear specifically cited in the Final Rejection is column 1, lines 33-49. This portion refers to on-line databases, but otherwise does not describe obtaining files from plural Internet sites.

3. Obviousness Rejections

The Final Rejection rejected claims 2-21 as being unpatentable under 35 USC 103(a) over Powell in view of Shear.

Claim 2

Claim 2 reads as follows:

2. A method of monitoring distribution of proprietary audio or image files on the Internet, comprising:

obtaining audio or image files from plural different Internet sites;

identifying plural of the obtained files having certain digital watermark data embedded therein, and decoding the digital watermark data therefrom;

by reference to said decoded digital watermark data, determining proprietors of each of said plural files; and

sending information relating to results of the foregoing monitoring to said determined proprietors;

wherein proprietors of audio or image files are alerted to otherwise unknown distribution of their audio or image properties on the Internet.

The combined teachings of Powell and Shear fail to disclose or teach all of the elements of claim 2.

As described above, Powell describes an image auditing process that requires an original image to be identified of which a subject image is suspected of being a duplicate. Once the original image is identified, Powell's auditing process determines whether or not the subject image is derived from the signed image.

Powell's embodiment cannot perform the process of "identifying plural of the obtained files having certain digital watermark data embedded therein, and decoding the digital watermark data therefrom" without first requiring that each of the original files be identified. Since the auditing method detailed in Powell's illustrated embodiment requires an original image file and its corresponding signature or signatures to be supplied for the auditing process, the auditing process preliminarily identifies the original image and owner of the image before determining whether the subject image was derived from the signed image. In comparison, claim 2 recites:

"by reference to said decoded digital watermark data, determining proprietors of each of said plural files".

Powell's embodiment also fails to teach: "sending information relating to results of the foregoing monitoring to said determined proprietors" as claimed. For this part of the claim, the Final Rejection cites col. 1 lines 12-49 and col. 5, lines 44-54. While Powell notes that "signatures identify the source of ownership of images", Powell does not disclose any method or mechanism for "sending information relating to results of the foregoing monitoring to said determined proprietors" as claimed.

Finally, Powell's embodiment fails to teach a method that alerts proprietors of "otherwise unknown distribution of their audio or image properties on the Internet." Again, Powell requires the original image to be identified before the auditing process can begin.

Since Shear is only cited as a reference that purportedly shows obtaining files from Internet sites, it does not compensate for the failure of Powell to disclose or suggest the elements of the claims as described above. Shear is only cited for one aspect of claim 2 pertaining to obtaining files from plural Internet sites. Thus, even if Shear shows this aspect of claim 2, it does not and has not been relied on to show other aspects of the claims. The combined teachings of Powell and Shear fail to disclose, teach or suggest all of the elements of claim 2.

Moreover, there is no suggestion in the art that would have led an artisan to (a) modify and supplement the teachings of Powell and Shear as needed to redress the shortcomings noted above, and (b) then combine the modified teachings in the manners necessary to yield the combination of claim 2. The statements to the contrary in the Final Action are not substantiated by the record. (The same shortcoming likewise applies to each of the claims dependent from claim 2, but for brevity's sake is not repeated for each.)

Claim 3

Claim 3 reads as follows:

3. The method of claim 2 including decoding the digital watermark data with reference to public key data.

In rejecting this claim, the Final Rejection refers to Powell at col. 6, lines 18-43. It is not clear how this cited passage of Powell teaches the elements of claim 3. This cited passage of Powell relates to normalizing a subject image using the original image. It fails to teach or suggest decoding a digital watermark with reference to public key data.

Since Powell's illustrated embodiment does not teach these elements, and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 3 obvious.

Claim 4

Claim 4 reads as follows:

4. The method of claim 2 including decoding the digital watermark data with reference to private key data.

In rejecting this claim, the Final Rejection refers to Powell at col. 6, lines 18-43, which is the same passage cited for claim 3. Again, this passage relates to normalizing a subject image using the original image. It fails to teach or suggest decoding a digital watermark with reference to private key data.

Since Powell's illustrated embodiment does not teach these elements, and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 4 obvious.

Claim 5

Claim 5 reads as follows:

5. The method of claim 2 in which the identifying includes performing a domain transformation on data from at least certain of said files, yielding transformed data.

In rejecting claim 5, the Final Rejection cites Powell at col. 5, lines 29-36. This cited passage refers to the types of manipulation that typically occur to a signed image. The point of this passage is to show that the presence of a signature should be verifiable in a signed image, even if it is manipulated. This particular passage and the Powell reference generally do not suggest that a domain transformation is used to identify files that have certain digital watermark data embedded therein as claimed.

Since Powell's illustrated embodiment does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 5 obvious.

Claim 6

Claim 6 reads as follows:

6. The method of claim 5 in which the identifying further includes performing a matched filtering operation on said transformed data.

In rejecting claim 6, the Final Rejection cites Powell at col. 6, lines 44-53. This paragraph in Powell refers to a process of comparing signature points in a subject image with stored signature points.

This process in Powell does not teach a matched filtering operation of domain transformed data as claimed. Instead, it is a comparison operation.

Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 6 obvious.

Claim 7

Claim 7 reads as follows:

7. The method of claim 5 in which said domain transformation is a 2D FFT transform.

In rejecting claim 7, the Final Rejection cites Powell at col. 5, lines 29-36. The Final Rejection acknowledges that Powell does not disclose a 2D FFT transform, but concludes that the use of this transform would have been obvious given the teachings of Powell.

As stated above for claim 5, Powell does not provide any teaching regarding the use of a domain transformation as part of the process of identifying files that have certain digital watermark data embedded therein. Powell's technique of auditing images operates on spatial domain image data without transforming the image data into another domain.

Since Powell does not use a domain transform to identify files with embedded digital watermark data, it is not clear how the claimed use of a 2D FFT for identifying files would be obvious in view of Powell.

Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 7 obvious.

Claim 8

Claim 8 reads as follows:

8. The method of claim 5 in which said domain transformation is a one-dimensional transform.

In rejecting claim 8, the Final Rejection again cites Powell at col. 5, lines 29-36. The Final Rejection acknowledges that Powell does not disclose a one dimensional transform, but concludes that the use of this transform would have been obvious given the teachings of Powell.

Since Powell does not use a domain transform to identify files with embedded digital watermark data, it is not clear how the claimed use of a one dimensional domain transform for identifying files would be obvious in view of Powell.

Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 8 obvious.

Claim 9

Claim 9 reads as follows:

9. The method of claim 8 in which the identifying further includes generating column-integrated scan data for at least one oblique scan through an obtained image, and performing a one-dimensional FFT transformation thereon.

In rejecting claim 9, the Final Rejection again cites Powell at col. 5, lines 29-36. This claim adds further elements to claim 8 that are not disclosed or taught in the cited art, such as "generating column-integrated scan data for at least one oblique scan through an obtained image...."

Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 9 obvious.

Claim 10

Claim 10 reads as follows:

10. The method of claim 2 in which the identifying includes computing power spectrum data relating to at least certain of said files.

In rejecting claim 10, the Final Rejection again cites Powell at col. 5, lines 29-36. This passage and Powell more generally do not teach computing a power spectrum as part of a process to identify files with digital watermark data embedded therein.

Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 10 obvious.

Claim 11

Claim 11 reads as follows:

11. The method of claim 10 including low-pass filtering said power spectrum data.

In rejecting claim 11, the Final Rejection again cites Powell at col. 5, lines 29-36. This passage and Powell more generally do not teach low pass filtering power spectrum data as part of a process to identify files with digital watermark data embedded therein.

Since Powell's illustrated embodiment does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 11 obvious.

Claim 12

Claim 12 reads as follows:

12. The method of claim 2 including analyzing a spectral characteristic of at least certain of said obtained files to identify the possible presence of digital watermark data therein.

In rejecting claim 12, the Final Rejection cites Powell at col. 6, lines 18-43. This passage and Powell more generally do not teach "analyzing a spectral characteristic of at least certain of said obtained files to identify the possible presence of digital watermark data therein." In fact, Powell's illustrated embodiment does not use any spectral analysis.

Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 12 obvious.

Claim 13

Claim 13 reads as follows:

13. The method of claim 2 including screening said obtained files to identify a subset thereof, and undertaking the decoding operation only for files in said subset.

In rejecting claim 13, the Final Rejection cites Figure 2 in Powell. Fig. 2 in Powell shows an example of a predetermined small neighborhood 28 and a large neighborhood 30 around a pixel 26. This figure and the accompanying text provide no teaching of screening obtained files to identify a subset thereof, and undertaking the decoding operation for files in said subset. Figure 2 pertains only to an embedding operation within a single image.

Since Powell's illustrated embodiment does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 13 obvious.

Claim 14

Claim 14 reads as follows:

14. The method of claim 13 in which the screening includes detecting a pattern in the file.

In rejecting claim 14, the Final Rejection again cites Figure 2 in Powell. As noted above, Fig. 2 is not related to screening files to identify a subset of files, and specifically, does not relate to detection operations. More specifically, Powell does not teach screening files to identify a subset of files as claimed by detecting a pattern in the file. Powell's auditing method operates on one image at a time without the claimed pre-screening operations and requires the user to identify an original before the auditing process can proceed to determine whether a subject image has been derived from a given signed image.

Since Powell's illustrated embodiment does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 14 obvious.

Claim 15

Claim 15 reads as follows:

15. The method of claim 2 in which the decoding includes performing at least one statistical analysis.

In rejecting claim 15, the Final Rejection again cites Powell at col. 6, lines 18-43. Claim 15 recites that the decoding process of claim 2, namely, "decoding digital watermark data therefrom," includes performing at least one statistical analysis. The cited passage refers to

normalizing a subject image relative to an original image. There is no teaching of a statistical analysis to decode digital watermark data.

Since Powell's illustrated embodiment does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 15 obvious.

Claim 16

Claim 16 reads as follows:

16. The method of claim 2 in which said obtaining includes automatic computer downloading of image or audio files, without specific human instruction of particular files to be downloaded.

In rejecting claim 16, the Final Rejection contends that Shear at col. 1, lines 33-49, provides the elements of claim 16. This cited passage of Shear refers to on-line public databases. It does not teach the automated downloading of files for use in identifying files having certain digital watermark data embedded therein.

Even assuming that automated downloading of files was known, the combined teachings of Powell and Shear fail to suggest all of the claim elements for the reasons set forth above for claim 2.

Claim 17

Claim 17 reads as follows:

17. The method of claim 2 in which the decoded watermark data provides a reference to a registry database, and the method further includes obtaining additional data from the registry database by use of said reference, said additional data identifying the proprietor of the file from which said watermark data was decoded.

In rejecting claim 17, the Final Rejection cites col. 1, lines 12-14 and col. 5, lines 44-54 of Powell. These particular passages and Powell in general fail to disclose or suggest the elements of claim 17.

Claim 17, for example, recites "the decoded watermark data provides a reference to a registry database." Further, the claim recites "obtaining additional data from the registry database by use of said reference...." Powell discloses that a signature is stored in a database in which it is associated with the original image. See Powell at col. 5, lines 21-27. However, Powell's illustrated embodiment first requires the original image to be identified, and then the signature or signatures associated with that image are obtained before analyzing a subject image to determine if it was derived from a signed version of the original image.

Powell's illustrated embodiment fails to suggest that any data decoded from a watermark in an image provides a reference to a registry database, and further, fails to suggest the use of such a reference to obtain additional data from the registry.

Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 17 obvious.

Claim 18

Claim 18 reads as follows:

18. The method of claim 2 including generating reports relating to results of said monitoring, and sending said reports to said determined proprietors.

In rejecting claim 18, the Final Rejection cites Powell at col. 1, lines 12-14 and col. 5, lines 44-54. These are the same passages cited for claim 17. Neither these specific passages, nor Powell generally disclose or suggest the elements of claim 18.

Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 18 obvious.

Claim 19

Claim 19 reads as follows:

19. A computer system programmed to receive image, video, or audio files downloaded from the internet, inspect such files for steganographically embedded data, identify proprietors of files by reference to said steganographically embedded data, and generate report data for relaying to such proprietors.

In rejecting claims 19-21, the Final Rejection appears to repeat the same rejection applied to claim 2, with the same citations to Powell. The combined teachings of Powell and Shear fail to render claim 19 obvious. As noted previously, Shear provides no teaching of steganographically embedded data, much less inspecting files for such data and identifying proprietors of the files by reference to said data.

Powell uses an embedded signature to determine whether a subject image has been derived from a signed image. While Powell notes that the signatures identify the source of ownership of images, the combined teachings of Powell and Shear fail to suggest a computer system programmed to identify proprietors of the files by reference to said steganographically embedded data and generate report data for relaying to such proprietors.

As explained above, Powell's illustrated embodiment requires the original image to be identified for each subject image before auditing the subject image to determine whether it was derived from a signed version of the original image. See Powell at col. 5, lines 44-46. Powell's database stores a signature along with the original image. See Powell at col. 5, lines 21-28. Powell's method of getting the stored signature points in the database is to identify the original image first, and then retrieve any signatures stored for that image.

Powell does not teach a computer system programmed to "identify proprietors of files by reference to said steganographically embedded data" as claimed. Powell teaches that the signature points in a subject image are compared with signature points stored for the image to determine whether the subject image was derived from the signed image. See Col. 5, lines 44-53. Further Powell does not teach a programmed computer system to "generate report data for relaying to such proprietors." Powell's auditing method concludes by determining whether a

subject image has been derived from a signed image identified by the user. Since Powell does not teach these elements and Shear adds no pertinent teachings for these elements, the combined teachings of Powell and Shear fail to render claim 19 obvious.

Again, as noted in connection with claim 2, there is no suggestion in the art that would have led an artisan to (a) modify and supplement the teachings of Powell and Shear as needed to redress the shortcomings noted above, and (b) then combine the modified teachings in the manners necessary to yield the combination of claim 19.

Claim 20

Claim 20 reads as follows:

20. Computer software stored on a physical storage medium, said software including code for receiving image, video, or audio files downloaded from the internet, inspecting such files for steganographically embedded data, identifying proprietors of files by reference to said steganographically embedded data, and generating report data for relaying to such proprietors.

Claim 20 is patentable for the same reasons as claim 19.

Claim 21

Claim 21 reads as follows:

21. A method of monitoring distribution of proprietary audio or image files on the Internet, comprising:

from at least one computer, automatically obtaining audio or image files from plural different Internet sites;

automatically identifying plural of the obtained files having certain digital watermark data embedded therein, and decoding the digital watermark data therefrom;

by reference to said decoded digital watermark data, determining proprietors of each of said plural files; and

sending information relating to results of the foregoing monitoring to said determined proprietors;

wherein proprietors of audio or image files are alerted to otherwise unknown distribution of their audio or image properties on the Internet.

Claim 21 is allowable for the same reasons as claim 2. In addition, claim 21 specifically recites "automatically identifying plural of the obtained files having certain digital watermark data embedded therein, and decoding the digital watermark data therefrom."

Powell states that the original images are identified for analysis of subject images before the auditing process can proceed. As such, Powell's illustrated embodiment does not teach "automatically" performing these claim elements.

IX. CONCLUSION

In view of the foregoing, applicant respectfully submits that a prima facie case of obviousness has not been established as to any of claims 2-21. Accordingly, the rejections of claims 2-21 should be reversed, and the application returned to the Art Unit for issuance of a Notice of Allowability.

Respectfully submitted,

DIGIMARC CORPORATION

Date: May 31, 2001

Digimarc Corporation
19801 SW 72nd Avenue, Suite 250
Tualatin, OR 97062
Phone: 503-885-8699

By _____
Joel R. Meyer
Registration No. 37,677

APPENDIX

PENDING CLAIMS

2. A method of monitoring distribution of proprietary audio or image files on the Internet, comprising:

obtaining audio or image files from plural different Internet sites;

identifying plural of the obtained files having certain digital watermark data embedded therein, and decoding the digital watermark data therefrom;

by reference to said decoded digital watermark data, determining proprietors of each of said plural files; and

sending information relating to results of the foregoing monitoring to said determined proprietors;

wherein proprietors of audio or image files are alerted to otherwise unknown distribution of their audio or image properties on the Internet.

3. The method of claim 2 including decoding the digital watermark data with reference to public key data.

4. The method of claim 2 including decoding the digital watermark data with reference to private key data.

5. The method of claim 2 in which the identifying includes performing a domain transformation on data from at least certain of said files, yielding transformed data.

6. The method of claim 5 in which the identifying further includes performing a matched filtering operation on said transformed data.

7. The method of claim 5 in which said domain transformation is a 2D FFT transform.

8. The method of claim 5 in which said domain transformation is a one-dimensional transform.

9. The method of claim 8 in which the identifying further includes generating column-integrated scan data for at least one oblique scan through an obtained image, and performing a one-dimensional FFT transformation thereon.

10. The method of claim 2 in which the identifying includes computing power spectrum data relating to at least certain of said files.

11. The method of claim 10 including low-pass filtering said power spectrum data.

12. The method of claim 2 including analyzing a spectral characteristic of at least certain of said obtained files to identify the possible presence of digital watermark data therein.

13. The method of claim 2 including screening said obtained files to identify a subset thereof, and undertaking the decoding operation only for files in said subset.

14. The method of claim 13 in which the screening includes detecting a pattern in the file.

15. The method of claim 2 in which the decoding includes performing at least one statistical analysis.

16. The method of claim 2 in which said obtaining includes automatic computer downloading of image or audio files, without specific human instruction of particular files to be downloaded.

17. The method of claim 2 in which the decoded watermark data provides a reference to a registry database, and the method further includes obtaining additional data from the registry database by use of said reference, said additional data identifying the proprietor of the file from which said watermark data was decoded.

18. The method of claim 2 including generating reports relating to results of said monitoring, and sending said reports to said determined proprietors.

19. A computer system programmed to receive image, video, or audio files downloaded from the internet, inspect such files for steganographically embedded data, identify proprietors of files by reference to said steganographically embedded data, and generate report data for relaying to such proprietors.

20. Computer software stored on a physical storage medium, said software including code for receiving image, video, or audio files downloaded from the internet, inspecting such files for steganographically embedded data, identifying proprietors of files by reference to said steganographically embedded data, and generating report data for relaying to such proprietors.

21. A method of monitoring distribution of proprietary audio or image files on the Internet, comprising:

from at least one computer, automatically obtaining audio or image files from plural different Internet sites;

automatically identifying plural of the obtained files having certain digital watermark data embedded therein, and decoding the digital watermark data therefrom;

by reference to said decoded digital watermark data, determining proprietors of each of said plural files; and

sending information relating to results of the foregoing monitoring to said determined proprietors;

wherein proprietors of audio or image files are alerted to otherwise unknown distribution of their audio or image properties on the Internet.